Digital Communication Policy

1. Introduction

Social media refers to any method of communication in the public forum including emails, forums, chat rooms, blogs, instant messaging and websites/apps such as Facebook, Instagram, Twitter, LinkedIn, TikTok etc. Any communication or "post" made on any platform will fall under the scope of this policy.

This document does not form part of a contract of employment and may be changed from time to time in line with current best practice and statutory requirements, and to ensure business needs are met. Staff will be consulted and advised of any changes as far in advance as possible of the change being made, unless the change is required by law.

2. Policy Aims

This policy sets out the standards and expectations of all persons acting on behalf of and/or associated with the organisation including staff and volunteers.

To clearly identify what language is and is not appropriate whether in a professional or personal capacity.

To ensure and protect the reputation of the organisation at all times.

To ensure it is understood any posts made whether on a personal platform or otherwise which could be considered as detrimental to organisational reputation may result in disciplinary action up to and including dismissal.

3. Responsibilities

3A Staff Responsibilities

To comply with the terms of this policy at all times, whether acting on behalf of the organisation or for personal purposes whether or not during working hours.

To be responsible for all social media account activity made in their name including access and posting, sharing, re-sharing, commenting or otherwise.

Report inappropriate digital communication immediately to a manager whether received from an internal or external source.

Staff members are encouraged to actively promote the good work of the charity while also maintaining a professional and considered approach when commenting on the work of the charity, its employees and members.

3B Line Manager Responsibilities

To ensure all staff understand their responsibilities and potential impact personal social media posting may have on their employment.

To deal with all reports of inappropriate digital communication seriously and timeously including any investigation, if necessary and any disciplinary action, if appropriate.

3C Organisation Responsibilities

To ensure fair, equal, reasonable and consistent treatment of all staff regarding any aspect of the implementation of this policy.

To ensure all those with line management responsibility are reasonably trained in the practical application of this policy.

To regularly review and update this policy in line with legislation and best practice.

4. Appropriate Language

Emails and social media are accepted as informal mediums whilst providing a permanent written record. Digital language can be stilted, abbreviated and conversational. Some may feel more comfortable emailing or posting information they would not necessarily say directly to another person or make a comment which is political or religiously motivated.

Inappropriate communication may be seen as harassment. Anyone communicating digitally must adhere to the following: -

- Personal data should not be transmitted digitally unless encrypted.
- Sending personal data digitally must comply with the organisations' Data Protection Policy.
- Digital information should not be retained for any longer than necessary and all should "clean" email accounts regularly.
- Appropriate language must be used at all times; any swearing will not be tolerated.
- Inappropriate messages are prohibited such as those which contradict, oppose or infringe on the values, purpose, ethos or principles of the organisation.
- Staff have the right to raise a grievance if they receive offensive digital communication from an internal or external source.
- Any access to or downloading of inappropriate material, such as pornography will not be tolerated.

5. Personal and Professional Social Media Posting

Information posted on public forums are by definition, public and not private. Staff and volunteers are not permitted to disclose confidential information relating to the organisation, service users, staff, volunteers, partners, suppliers or stakeholders on

any public forum. It is also prohibited to post any comments on organisations, people or events which could potentially bring the organisation into disrepute.

When posting, commenting or sharing material relating to the organisation, its business or otherwise, appropriate language must be used at all times. Be professional. Make sure you are always seen to act in an honest, accurate, fair and responsible manner at all times.

To minimise potential risk, all are expected to: -

- Keep all profiles secure and password protected.
- Not disclose passwords to any other person and not allow other persons to post on their account.
- Refrain from posting, commenting or sharing any inappropriate digital communication, particularly relating to the organisation or any matter which could be considered as discriminatory towards or against any person or persons.
- Do not cite or reference members, guides, or interpreters without their approval.
- If quoting, or publishing a photograph or video of, a member, interpreter, guide, volunteer or a Deafblind Scotland employee, approval by that individual via a consent form must be obtained.
- Publishing data regarding member's private details is forbidden except if approval has been given by the member, the services manager and your line manager.
- You must always alert your manager if you think you may have made a mistake.
- Respect copyright when linking to images or other online material.
- When posting a video, or providing a link to a video, the administrator must make sure (when possible) the video is subtitled so it is accessible to those with a hearing impairment.
- Consider if the information you are posting requires permission from a third party organisation and seek this when appropriate
- Understand that any digital communication on a public forum can and will result in disciplinary action if deemed inappropriate and/or could have a detrimental impact on the organisational reputation.
- Staff should obtain permission from their line manager before embarking on a public campaign using social media and using social media guidance.

Only nominated administrators have the authority to update Deafblind Scotland social media accounts. The Information Officer, Fundraising and the Senior Management Team are the lead administrators responsible for updating principle Deafblind Scotland social media sites. Sub groups created with the explicit intention of raising the profile their respective departments through Twitter should also adhere to the following administrator rules and guidelines.

Designated administrators will hold the necessary passwords to log into social media sites and should keep them private.

Any update to Deafblind Scotland social media accounts must be approved by the chief executive, or an administrator appointed by the Chief Executive, before it is published.

The language used by the administrator on Deafblind Scotland social media sites should be accessible to all.

Staff must be aware at all times, while contributing to the organisation's social media activities, they are representing the organisation.

If staff work related activity/volunteering duties on social media (for example, giving opinions on their specialism or the sector in which the organisation operates), they should include on their profile a statement such as: "The views I express here are mine alone and do not necessarily reflect the views of the organisation."

6. Data Monitoring

All organisational accounts such as email and social media may be monitored for the purpose of quality control, service delivery and to identify breaches of this policy. Should potential disciplinary action be considered, an investigation will take place with the investigating officer being provided with full access to the email account.

During any period of leave such as annual, sick, maternity, paternity etc., accounts may be accessed to ensure continued service delivery.

The organisation reserves the right to inspect, copy, store, and disclose the contents of digital communication to prevent or correct improper use, satisfy a legal obligation or ensure proper operation of the digital communication facilities.

7. Personal Emails

Personal emails should not be sent from organisation email accounts. The purpose of organisation email accounts is for staff to send and receive information on behalf of the organisation and not for personal reasons.

Any personal use of organisation email accounts may result in disciplinary action especially where it is deemed abuse of the email account has taken place.

8. Personal Grievances

Personal grievances or disputes linked with the charity, its employees, or members - either directly or indirectly - must not be published on any social media platform, or linked to a Deafblind Scotland social media platform.

9. Personal Relationships

In accordance with the Scottish Social Services Council's Codes of Practice (in particular section 5) Deafblind Scotland employees must refrain from forming personal relationships with members through social media platforms.

Scottish Social Services Council's Codes of Practice Section 5:
As a social service worker you must uphold public trust and confidence in social services.

In particular you must not:

- Abuse, neglect or harm service users, carers or colleagues.
- Exploit service users, carers or colleagues in any way.
- Abuse the trust of service users and carers or the access you have to personal information about them, or to their property, home or workplace.
- Form inappropriate personal relationships with services users.
- Discriminate unlawfully or unjustifiably against service users, carers or colleagues.
- Condone any unlawful or unjustifiable discrimination by service users, carers or colleagues.
- Put yourself or other people at unnecessary risk; or,
- Behave in a way, in work or outside work, which would call into question your suitability to work in social services.

10. Photos and Videos

Photos and videos which could bring the organisation into disrepute must not be posted, published, or linked. If in doubt please seek advice from your line manager.

11. Declaration by association

Social media activity is open to public scrutiny and consequently Deafblind Scotland employees should remain aware of potential repercussions of "liking", "following" "befriending" or "commenting" on groups, individuals or movements which have the ability to bring the charity into disrepute through association.
If an employee's social media account is linked to Deafblind Scotland they should have a disclaimer which states "all views and opinions expressed are my own"

12. Security and Identity theft

Social networking websites allow people to post detailed personal information which can form the basis of security questions and passwords.
Staff must be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. At all times staff must keep their password confidential.

13. Device Security

All devices including computers, laptops and mobile phones provided by the organisation will be security protected with software updated as and when necessary. All users of organisational devices must comply with the security protection such as ensuring password access.

Passwords must be kept confidential and should not be shared with anyone, including colleagues with the exception of the line manager and/or IT person(s). Passwords should be changed regularly, at least once a month using an appropriate word or phrase, upper and lower case and at least one number.

Anyone using their own, personal device for work purposes, must comply with the terms of this policy and have up to date, valid virus protection software installed on the device at their own expense. Failure to comply with this term could result in risk to the organisation and disciplinary action.

14. Data Protection Act 2018

The organisation will treat all personal data in line with obligations under the current data protection regulations.